

Disaster Strikes! Is Your Business Ready? Disaster Preparedness for Mid-Sized Firms



www.yankeegroup.com

by Gary Chen | February 2008

Abstract

Mid-sized businesses have long struggled to protect their IT systems. Many firms are inadequately protected and mistakenly think that a disaster is rare and won't happen to them anytime soon. This custom Yankee Group Report uses customer interviews, statistical data and Yankee Group SMB survey results to examine disaster recovery (DR) issues for mid-sized businesses. There is a lot of confusion and misunderstanding regarding what disaster recovery encompasses and how to effectively implement it. This Report explores common minor and major disaster scenarios, shows that they are far likelier than most people think, and explains how they can affect a business. This Report also clarifies what true disaster recovery means and how backup and high availability are not true DR solutions. We study the newest technology trends, such as virtualization and storage replication, which make powerful DR solutions attainable and affordable even for mid-sized businesses. Finally, a list of practical recommendations and DR strategies is presented as a guide to improving any mid-sized firm's level of protection.

Many firms are inadequately protected and mistakenly think that a disaster is rare and won't happen to them anytime soon.

This custom publication has been sponsored by VMware.

© Copyright 2008. Yankee Group Research, Inc. All rights reserved.

This Yankee Group Report is published for the sole use of Yankee Group clients. It may not be duplicated, reproduced or transmitted in whole or in part without the express permission of Yankee Group, Prudential Tower, 800 Boylston Street, 27th Floor, Boston, MA 02199. For more information, contact Yankee Group: info@yankeegroup.com; phone: 617-598-7200. All rights reserved. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice.

Table of Contents

I.	Introduction	3
II.	Disaster Scenarios	3
	Hardware Failures	4
	Software Errors	4
	Power Outages	4
	Circuit Failures	5
	Natural Disasters	5
	Human Error	6
	Fire	6
	Odds and Ends	6
III.	BCDR Maturation Curve	7
	Backup	7
	High Availability	8
	Disaster Recovery	8
	Business Continuity	8
IV.	Disaster Recovery Strategies	9
V.	Conclusions	11

I. Introduction

The results of the Yankee Group *Anywhere Enterprise—Small and Medium: 2007 US IT Infrastructure Survey* and the *Anywhere Enterprise—Large: 2007 US IT Infrastructure Survey* show that mid-sized firms with 100 to 999 employees are concerned with protecting their IT systems (see Exhibit 1).

Exhibit 1

Business Protection Is Top of Mind for Mid-Sized Firms

Source: Yankee Group *Anywhere Enterprise—Small and Medium: 2007 US IT Infrastructure Survey*; *Anywhere Enterprise—Large: 2007 US IT Infrastructure Survey*

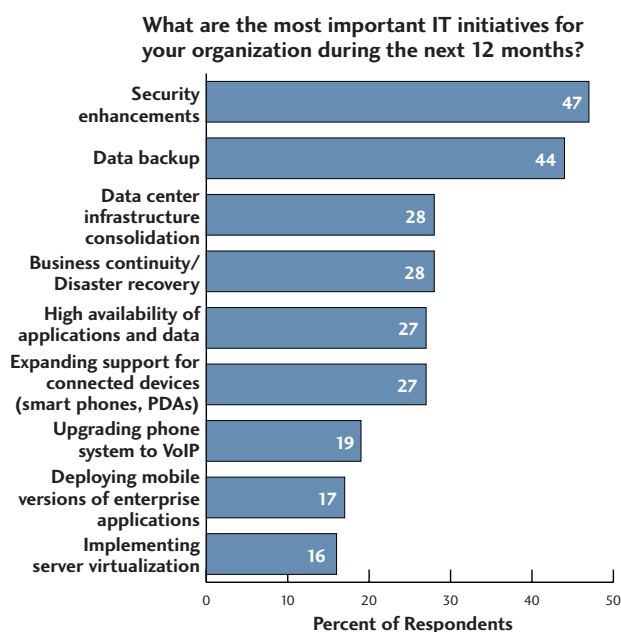


Exhibit 2

Mid-Sized Companies Interviewed

Source: Yankee Group, 2008

	Type of Business	Number of Employees	Number of IT Staff	Number of Locations	Number of Physical Servers
Maxim Group	Financial Services	425	3	5	50
VT Specialized Vehicles	Manufacturing	1,100	5	6	20
Moldflow	Software Developer	350	10	20	50
Los Angeles Valley College	Education	600	8	10	500
Bowdoin College	Education	850	36	1	50
Exponential Interactive	Online Advertising Network	120	11	7	60

Businesses' reliance on IT systems and digital data has never been greater. The 2007 *Best's Underwriting Guide* by A.M. Best found that only 6% of companies that suffer catastrophic data loss survive while 43% never reopen and 51% close within 2 years of the disaster. *Best's Underwriting Guide 2007* also found that 93% of the companies that did not have their data backed up in the event of a disaster went out of business.

SMBs' prioritization of disaster recovery, backup and high availability for 2008 shows that businesses understand the risks to their business and the value of protection. However, many organizations still errantly think that backup is a sufficient disaster recovery plan. But, mid-sized enterprises are at the most risk to disaster and are more likely to rely strictly on backup as a disaster recovery plan.

The needs and resources of mid-market firms are unique. Mid-sized companies must work with limited finances infrastructure and human resources. Robust disaster recovery used to be affordable and manageable only by large enterprises. Mid-sized enterprises relied more on backup than on a formal disaster recovery plan. As businesses' reliance on IT has grown, backup has increasingly shown its weaknesses. However, the introduction and maturation of several key technologies, such as virtualization, have brought affordable and easily implementable DR to small and mid-sized companies. But as Exhibit 1 shows, SMBs don't always equate virtualization with DR because awareness of the many virtualization applications is just starting to grow. For this Report, Yankee Group collected data specifically for companies with 100 to 1,100 employees and interviewed six companies from different industries in this range (see Exhibit 2).

II. Disaster Scenarios

Planning for a disaster can be a daunting task. Businesses often ask "What scenarios should I prepare for?" and "How likely is it that it will happen to me?" When one thinks of disasters, big events such as Hurricane Katrina or 9/11 are the first come to mind. But if we look at the ultimate consequence of a disaster—downtime—we can see that any event, large or small, can have the same effect on IT infrastructure. Comdisco, a provider of disaster recovery services, lists hardware problems as the number one cause of disaster, followed by power outages, hurricanes and floods (see Exhibit 3 on next page).

Let's take a brief look at some common disaster causes and what effect they can have on a business.

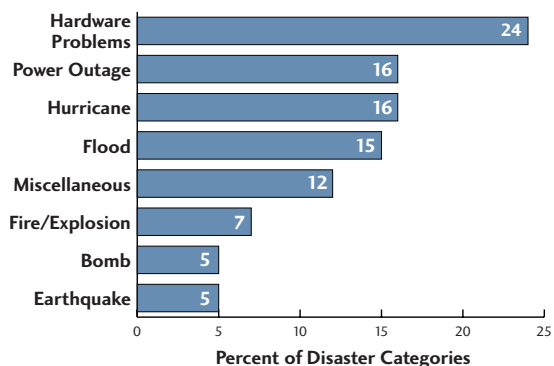
Hardware Failures

Hardware fails. It's a fact of IT. The most vulnerable components have moving parts, such as hard drives, which also happen to hold a company's most valuable and irreplaceable asset—data. Replacing hardware can be a laborious process because you must physically obtain the component, which may take a day or two if you don't regularly stock spares, then visit the site to replace it.

Exhibit 3

The Most Common Causes of Disasters

Source: Comdisco, 1999

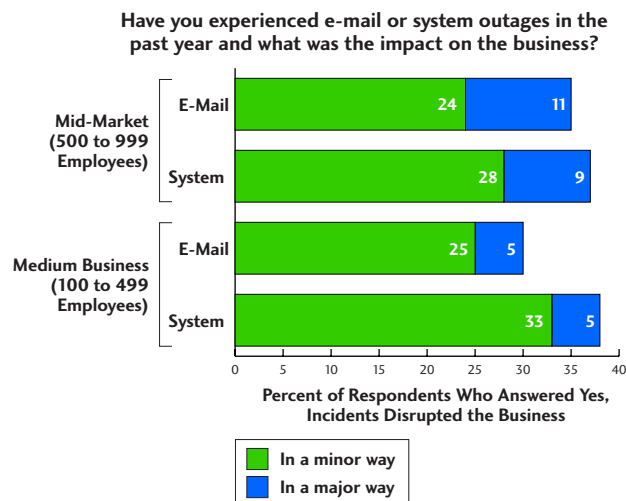


Note: Disaster categories out of 320 recoveries supported.

Exhibit 4

E-Mail and System Outages

Source: Yankee Group Anywhere Enterprise—Small and Medium: 2007 US IT Infrastructure Survey, Anywhere Enterprise: Large: 2007 US IT Infrastructure Survey



Software Errors

Software has become increasingly large and complex. With complexity comes more room for errors. Systems that have been running fine for a long time can run across a software bug unexpectedly and go down. Fixing the problem can take a fair amount of detective work by both IT and the ISV. In the case of Maxim Group, a financial services firm, a hard drive failure in its Exchange Server sparked the incident. It had a RAID 1 mirror and switched to that in a matter of minutes. However, the Exchange software would not come back up. It took 4 hours before service was restored and Microsoft engineers had to do deep debugging to track down the problem. The cause was eventually found to be a setting that got inadvertently changed during the incident, but how it got changed is still a mystery. For uptime statistics on mid-sized firm's e-mail systems and servers, see Exhibit 4.

Power Outages

IT systems all rely on electricity. Without it, systems must shut down. Although uninterruptible power supplies (UPS) will get systems through brief outages, only a costly backup generator can provide the power for an extended outage. According to Michael Hyland, vice president of engineering services at the American Public Power Association, although power reliability in the United States is overall very good, outages do happen.

“The ASAI (average system availability index) for the United States is around 99.999%, which is a tremendous achievement in reliability very few other industries have achieved. That means on average, a customer will experience one power interruption of a little more than an hour per year. However, those are average figures for the entire nation across all customers. Customers need to prepare for outages of several hours and even days, which aren't all that uncommon, especially if you are in a winter/electrical storm or hurricane region. The most ingenious engineering still can't overcome Mother Nature. Bad weather is going to cause outages, not to mention all sorts of other random events, which can include squirrels, a car that hits a pole, and trees. There are things you just can't control.”

Certain areas of the United States have also had power supply problems in the recent past. Most notable is California with its infamous rolling blackouts during the early 2000s and as recently as August 2005. Parts of Texas also implemented rolling blackouts during April 2006 due to abnormally high temperatures. Other regions of the country implement brownouts, where the voltage is reduced to customers during power emergencies. Brownouts can severely affect electronic equipment not protected with an UPS or voltage regulation device. Jorge Mata of Los Angeles Valley College was located in the region of California affected by the power crises. Mata said:

“Basically you have to restore and operate your systems from an alternate location that has power. Obviously, that site is usually pretty far away and it isn’t practical to physically move systems. Moving an interconnected web of storage and servers to another set of infrastructure is a huge challenge. These things just weren’t designed for that kind of mobility and that is exactly the problem that virtualization solves.”

Circuit Failures

As businesses rely more heavily on the internet to transact business and link together branch offices, remote workers, customers and business partners, the WAN connection becomes more important than ever. A single pipe may be a company’s only link to the outside world. If this pipe goes down, crucial networking functions come to a crashing halt. Although most business lines are pretty reliable, outages are not all that uncommon (see Exhibit 5). Moldflow, a plastics manufacturing software company, has about 20 branch offices each with a T-1. Dominic Yu, Moldflow’s system administrator, said about once a month they have a T-1 outage in one of the offices, lasting from 4 to 20 hours. During that time, that remote office is effectively cutoff. Scott Clayton from VT Specialized Vehicles Corporation said in the past year they’ve had about two WAN outages each lasting a couple of hours, cutting off both voice and data. “Without the WAN line, you can’t make phone calls, get e-mails or do any kind of electronic transaction,” Clayton said. “You’re pretty much unable to communicate with the outside world and effectively dead in the water.”

Natural Disasters

Nothing man-made can withstand the forces of nature. In certain regions of the country, natural disasters are not a question of if, but of when. The main headquarters of VT Specialized Vehicles is located in North Carolina, right in the heart of Hurricane Alley. “We know a hurricane is going to be coming along at some point; it’s inevitable,” Clayton said. “At the worst, you’re looking at physical damage to facilities and systems, or flooding. At minimum, it will knock out power and your network circuit. Even if power and network stay up, just the fact that you don’t have physical access to your system may prevent you from doing a crucial operational task” (see Exhibit 6).

Exhibit 5 Network Outages

Source: Yankee Group Anywhere Enterprise—Small and Medium: 2007 US IT infrastructure Survey, Anywhere Enterprise—Large: 2007 US IT infrastructure Survey

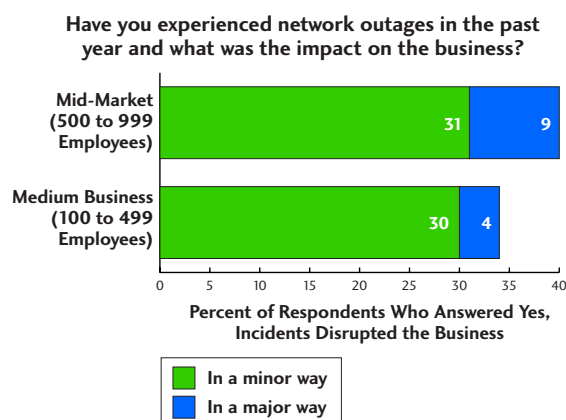
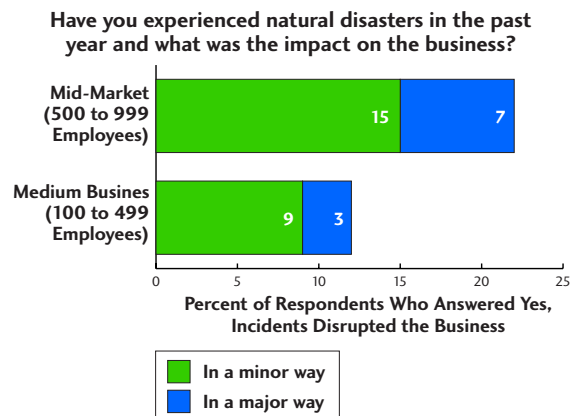


Exhibit 6 Natural Disasters

Source: Yankee Group Anywhere Enterprise—Small and Medium: 2007 US IT infrastructure Survey, Anywhere Enterprise—Large: 2007 US IT infrastructure Survey



Human Error

Although we would all like to have perfectly laid out policies and rigid change management procedures, in the real world this isn't the case, particularly in a mid-sized company where IT resources may be limited. Jorge Mata of Los Angeles Valley College experienced this with his Exchange Server:

“Someone had misconfigured a setting and it was replicating corruption throughout the organization's Exchange servers. The server would work for awhile, then go down again. We had a back-up server, so we were constantly restoring one while the other was running and cutting over back and forth for like a week before we figured it out. During the constant cutovers, the Exchange Server was unreachable for brief periods of time.”

Fire

In addition to the Exchange Server issue discussed above, Jorge Mata has had the unenviable honor of experiencing a fire caused by arson twice in 2 years:

“While damage from heat and water is obvious, fires disrupted our business in more ways than that. During the cleanup and investigation process, which can take a long time, they would not allow us into the facilities, so we could not get access to the systems to find out why they were down. Eventually we were able to get in there and get to work. We managed to repurpose some hardware to start restoring from backup, while we waited for new hardware to arrive. It took us about a day to actually restore the systems, but as a whole, we weren't really back on our feet for a week. Another long-term effect is that we had our servers professionally refurbished and cleaned from the water damage. The systems worked for awhile, but even with the cleaning all the systems grew mold after a few months, which acted like insulation and caused the system to overheat. After 3 to 4 months, almost every system from the fire had that problem and died.”

Odds and Ends

The list of other potential disasters could fill pages. Maxim Group, located in Manhattan, had its facilities evacuated because of a major steam pipe explosion. Maxim Group also had an AC technician fail to turn on the unit after servicing it, causing the temperature to rise to 128 degrees F, which caused four hard drives to fail.

Los Angeles Valley College was shut down due to the Los Angeles riots of 1992. “It was too dangerous to go anywhere,” said IT admin Mata. “Just having physical access to systems can be crucial, and no one is going to risk their life to get to the data center. Political events like these happen all the time and you have to be ready for anything. It's not unlikely that there could be a pandemic in the near future, and I have to figure out what to do if something like that happens.”

Clearly, the world can be unpredictable and disasters come in all shapes and sizes. It is not a question of if a disaster will happen, but merely when. These customer stories are far from unique. Businesses must be prepared for a disaster, but many lack understanding of the various approaches and their effectiveness. Is having a solid backup good enough? In the next section we explore the various approaches and examine their effectiveness (or lack thereof) for today's time-critical DR requirements.

III. BCDR Maturation Curve

What is disaster recovery? Is backup considered DR? Not exactly. While having backups is one component of a disaster recovery plan, a backup in itself is not robust enough to be considered true DR. The various levels of protection are shown in the BCDR maturation curve in Exhibit 7. The curve begins with the basic level of protection, data backup. As you move up the curve, the level of protection increases, but so does the cost and complexity of the solution. Each higher level of the curve is a superset of the lower components. We can also see how new technologies such as virtualization and networked storage are reducing the cost and complexity of effective disaster recovery. Let's examine the different parts of the curve and the protections they offer.

Backup

All good contingency plans start with having a good solid backup of data. Although systems and applications can be reinstalled and reconfigured, data cannot be rebuilt out of thin air. The key to having a good backup is to make sure that the data has integrity and can be successfully restored. This isn't always as easy as it seems, especially with tape (see Exhibit 8). Rob Cambra, an IT administrator at online advertising network Exponential Interactive, had such an issue several years ago. "Our backup admin didn't follow procedures correctly and

when he thought he was doing a backup, he actually wasn't writing any data," he said. "When we tried to restore a database, we found out all the tapes were blank. Imagine our surprise!

We eventually found the backup, but had to hire a consultant to reconstruct the [database] DB manually, some of which required going back to paper records." The other key with backup is storing a copy off-site. Tapes stored in the same location as the original data expose you to unnecessary risk. If something happens to that site, both copies would be lost. Tape is still the most prevalent backup mechanism because no other medium can store and archive large amounts of data more cost-effectively. Tapes are also easy to ship to off-site locations.

Although many companies think having a backup is all that is needed to restore their systems, most companies that actually try to do so encounter many obstacles. First, a company may have to wait for replacement hardware to arrive. Then it must reinstall the OS and applications and reconfigure the software. This can be a time-consuming task because restoring every setting to exactly the way it was before can be difficult, especially with systems that were initially configured a long time ago. Before a company can begin restoring the data, the back-up tapes must be located and retrieved from the off-site location. Reading the tapes can take hours, even days depending on the amount of data to be restored, as tape medium is relatively

Exhibit 7

The BCDR Maturation Curve

Source: Yankee Group, 2008

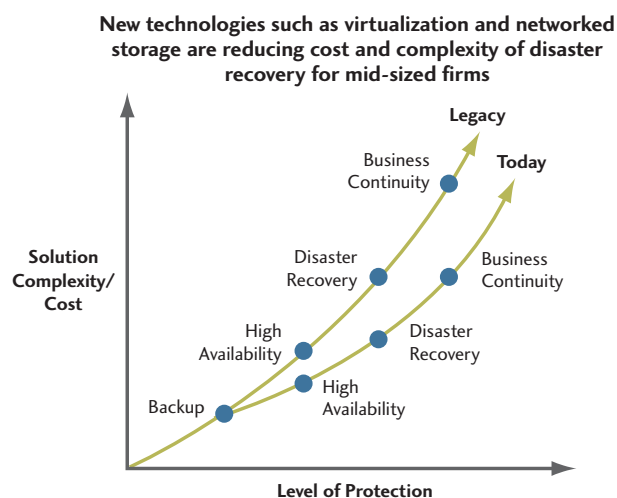


Exhibit 8

Tape Backup Pros and Cons

Source: Yankee Group, 2008

Pros	<ul style="list-style-type: none"> • Unbeatable capacity/price ratio • Convenient for archiving • A well-understood, mature technology
Cons	<ul style="list-style-type: none"> • Relatively slow read and write speeds • Poor at capturing complete system states, most suitable for data only • Have to physically ship tapes off-site for maximum protection • Must physically find and obtain off-site tapes to restore • Error prone, and not always reliable at recovery • Difficult to restore on dissimilar hardware

slow compared to disk. Assuming that the data on the tapes is good, the system should be functioning again. Scott Clayton from VT Specialized Vehicles experienced this procedure before his company adopted better DR technology. Clayton said:

“We had to wait for a server to be overnighted to us before we could reload the operating system and the applications. Then we began reading in the data from our tapes, which took us a full day to do. Eventually we got the system back and running, but the whole procedure took us several days. Although we still do tape backup today, it is for archiving and as a last resort only, not for disaster recovery. It just takes too long to restore a system from a traditional backup. Now we use a combination of app-level replication, VMware ESX, and highly redundant systems and networks to do our DR. What we are trying to do is create a generic infrastructure layer that we can layer our services and applications on top of. The services and apps are highly mobile blocks of computing that can operate on any part of our infrastructure.”

High Availability

Although backups protect data, data is useless without the application or server to access it. Thus, these systems must be made highly available to make use of the backup. High availability (HA) systems adopt the philosophy of redundancy. HA systems will typically have two of everything, such as power supplies and network cards. Tim Antonowicz of Bowdoin College uses HP blades to provide him with good resiliency. “All the typical components have redundancy such as the power supply, but also all the paths inside the blade chassis are multipath, and we also have multipath connections to our NetApp filer,” he said. “This kind of system gets us through your typical hardware or network failures.”

Clustering or load balancing is the software version of hardware redundancy. This type of architecture groups several computers together so that if one fails the others can pick up the load. It may be that all the nodes are always active, or the secondary nodes can be in passive standby mode, only to be used if the active server goes down. There is also load balancing type architecture, where a frontal load balancing machine distributes requests to a group of servers behind it. Most of these technologies are implemented on the same LAN,

so it still does not protect against site-wide disasters. Generally these solutions are fairly complex, require a high level of expertise to implement, and can be costly. It also requires constant cluster configuration maintenance, which can introduce errors. John Michaels from the Maxim Group looked at Microsoft clustering for his Exchange Server. “It was just too complicated for us as a mid-sized business to learn and manage it, he said. “I just don’t have the resources for it. Plus, most clustering solutions require centralized storage which we don’t have yet.”

Disaster Recovery

What makes a true disaster recovery solution is the ability to restore full systems quickly, in a matter of hours or even minutes, on available computing resources which may be local, but may also be remote if the situation dictates. True disaster recovery must allow recovery from site-wide disasters, such as a hurricane. In such a scenario, the primary site may be completely down, due to a lack of power and network connectivity. A secondary site located in a non-affected area would be used to restore services until the primary site comes back online. Jorge Mata of Los Angeles Valley College has a remote DR site for such scenarios. “Most of our servers are now virtual,” Mata said. “We use asynchronous replication to replicate both our data and virtual machines to this site, which has a number of standby servers. If we need to light up the site, we just fire up the virtual machines and all the systems are back up and running with the latest data.”

Business Continuity

Business continuity goes beyond IT infrastructure and applications to include all the processes that keep a business running, from people, alternate worksites and business processes to non-IT systems such as paper records. Full business continuity is beyond the scope of this Report, but readers would be advised to plan for disasters beyond just recovering IT systems. Plans for mid-sized companies may not be the full-blown, highly detailed plans devised by *Fortune 500* firms, but even basic planning will go a long way.

IV. Disaster Recovery Strategies

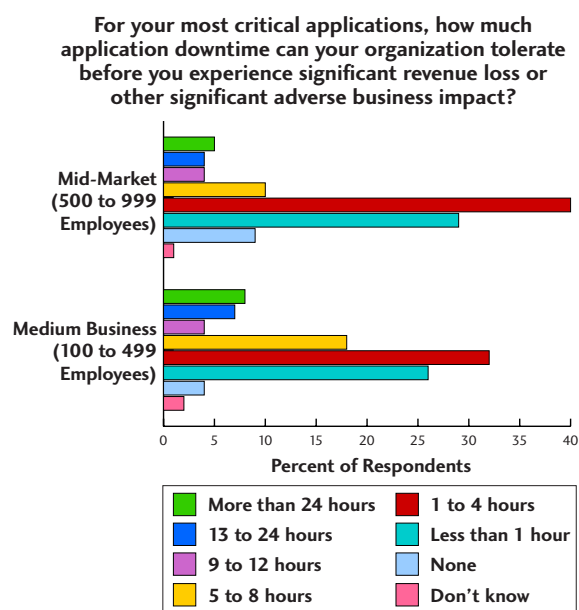
Aim for the quickest recovery time objectives (RTOs) possible. If an IT administrator interviews different users, they will tell you that their system is the most critical and they can't live with even a minute of downtime. Most of the time this simply is an exaggeration. Even if it were true, it would be impossible to achieve. Data from the Yankee Group *2006 US Small & Medium Business Storage Survey* indicates that most companies can tolerate about 1 to 4 hours of downtime for their most critical applications (see Exhibit 9). Generally, RTOs on the order of hours were considered a realistically achievable and affordable goal for mid-sized companies. However, as the speed of business increases, RTOs on the order of hours can still significantly disrupt a business, and this downtime tolerance will decrease further as time goes on.

Businesses must have the mind-set that DR must be accomplished in less than 1 hour in order to fully protect the business. Until virtualization, RTOs of less than an hour were considered attainable only for the largest companies with large budgets. Virtualization encapsulates entire systems into a few files, which are easily movable with standard methods.

Exhibit 9

Most Companies Can Tolerate 1 to 4 Hours of Downtime

Source: Yankee Group 2006 US Small & Medium Business Storage Survey



Virtual machines are not tied to specific hardware and can be booted up on any virtualized x86 server. Tim Antonowicz of Bowdoin College said, "Pre-virtualization it took about 2 to 4 hours for me to restore any given system because I had to reinstall the OS and apps. Data restoration was pretty fast for us as we have disk-based backups and also snapshots on our NetApp that we can use as well. Now using VMware, I can get almost any system back up in about 15 to 20 minutes. I recover the virtual machines, which are just files, using snapshots or some other method and boot them back up."

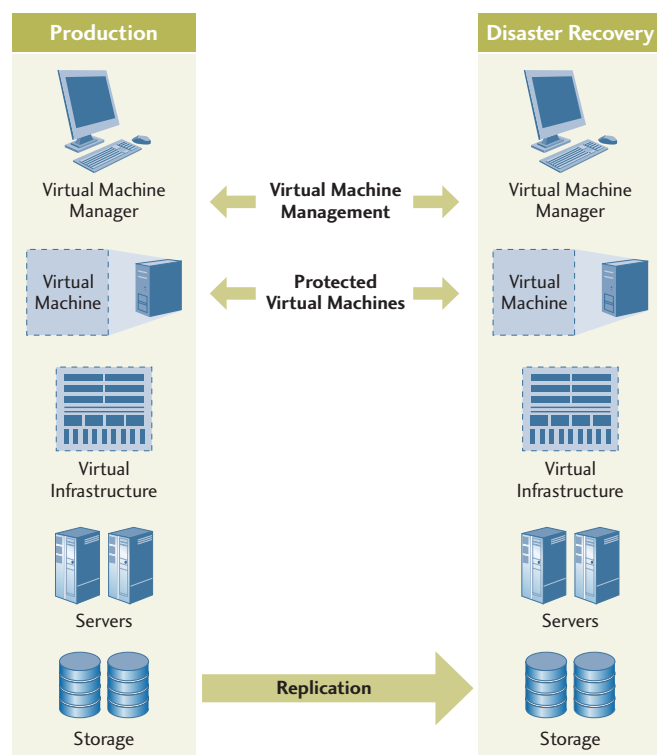
A secondary DR site is critical. Although resiliency within a system or LAN will get you through the small everyday failures, it won't be enough for a larger disaster that affects an entire site. Just as back-up tapes should be stored off-site, systems should be recoverable to remote locations. Although building a dedicated secondary DR site can be expensive and therefore unaffordable for many mid-sized companies, virtualization technology can put a robust, cost-effective DR plan within reach. Through server consolidation, virtualization can enable a company to reuse existing infrastructure for DR purposes. Most mid-sized firms have multiple locations or branch offices and virtualization allows easy reuse of excess capacity at these sites for DR. With the consolidation and efficiency allowed by virtualization, excess capacity may already exist or can be easily attained with just a few servers. Additionally, the cost savings realized by implementing virtualization can free resources to invest in additional DR technology, such as networked storage that can be replicated.

Establish multiple recovery points. Just as you store weeks or months of backups, you want to be able to restore your systems to multiple points in time. Software errors, data corruption and misconfigurations can go undetected or undiagnosed for hours or days. Being able to roll back the clock is a powerful tool in an emergency. Many storage devices provide snapshot capabilities for data with minimal capacity overhead. Snapshots can be taken of virtual machines as well, allowing you to restore entire servers to the exact state they were in. Companies must examine the risk of each system along with the storage resources available to establish a reasonable recovery point objective (RPO) that will offer the necessary protection.

Replicate your data. Asynchronous data replication is becoming a powerful tool in disaster recovery. This allows a secondary remote storage device to be always in sync with the primary, eliminating the need for time-consuming data restoration in the event that the DR system needs to be started. With the growing amount of digital data, trying to copy it after a disaster could be impractical, especially over a WAN link, which could be down as well. Replication is most often done at the block level on the storage device, but many applications such as databases have built in application-level replication that can also be used. Rob Cambra of Exponential Interactive recommends replicating data at least twice. “I try and have three copies of all my data,” he said. “I replicate once to a device on the same LAN and once to a remote location over the WAN. This gives me a high level of protection and flexibility if I ever need to use one of the replicas.”

Exhibit 10 A Replicated, Virtualized Infrastructure

Source: Yankee Group, 2008



Replication paired with virtualization can provide a powerful and cost-effective DR architecture (see Exhibit 10). Virtual machine images and data on a centralized networked storage device (iSCSI or NAS) are replicated to a remote storage device over the WAN. Both networked storage devices have standard x86 servers connected that can easily boot any virtual machine quickly.

Professional facilities. If your company can afford it, professional hosting facilities can offer many benefits that may otherwise be impractical for mid-sized firms to implement themselves. Many are located in reinforced buildings that can survive most natural disasters. Power outages become less of an issue as back-up generators are provided for the entire facility. These facilities also have multiple network providers, ensuring that connectivity is always on. Other systems such as cooling and fire suppression are also redundant and more reliable.

Test, test and test again! Nothing will work out the kinks in a system like real-world testing. You must have confidence that your disaster recovery procedures will work when that unforeseen event happens. The chaos that inevitably follows a disaster is certainly not the time to put a system to the test. Yankee Group recommends running DR tests every quarter or biannually to ensure that your protection mechanisms will actually protect you when you need them most.

Virtualization is already a proven tool for software testing and development and this applies equally to DR testing. Because provisioning, cloning, snapshotting and rolling back virtual machines is so quick and simple, virtualization significantly simplifies the ability to test DR plans. Multitiered virtual machines can be quickly provisioned and set up to be put through a test to ensure recoverability. Periodic and frequent DR testing can be done much more easily in a virtualized environment without the resource costs and disruption required in a physical one.

Get help from a qualified partner. Technology partners are crucial to the success of an SMB. Most SMBs enlist some sort of help in implementing and managing their IT systems. DR can be a challenging and complex task, and the advice and experience of an expert will ease the process greatly. Look for a partner that takes the time to get to know your business and can offer solutions tailored for your needs. As virtualization becomes the de facto standard for infrastructure, it will be crucial to also find a partner highly qualified in all aspects of virtualization.

The time to virtualize is now! Virtualization is the future of infrastructure. Virtualization will not only revolutionize DR, but also every aspect of IT infrastructure. What was once a cutting-edge technology is now proven, mature, and affordable even by small and mid-sized firms. John Michaels from Maxim Group is planning to implement VMware's Virtual Infrastructure product in 2008. "Virtualization is a no-brainer. It completely changes the way you do infrastructure," he said. "So far I've just used the 30-day trial version and during those 30 days it has already paid off, saving me from a few disasters. That convinced me and I've made it a priority for us to move to a virtualized environment in the 6 to 12 months." With all the benefits that virtualization clearly brings to IT, the time to virtualize is now.

V. Conclusions

The world can be a chaotic, random place. Disasters and the unforeseen happen with frightening regularity. Some are small and regular occurrences such as a hard drive failure or power outage. Some are major catastrophes such as Hurricane Katrina or 9/11. And some are unusual and unexpected such as the Manhattan steam pipe explosion. The fact is that any of these incidents, large or small, can cause your system to go down. Individually, the risk of each type of incident occurring is fairly low. Combined however, the risk of experiencing some sort of disaster is quite likely, almost inevitable. With the availability and price points of powerful technologies tailored especially for mid-sized firms, such as blade servers, networked storage, replication, and virtualization, achieving better uptime and business protection has never been easier or more affordable. So when that next disaster strikes, will you be ready?

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

Prudential Tower
800 Boylston Street
27th Floor
BOSTON, MASSACHUSETTS 02199
617-598-7200 phone
617-598-7400 fax
info@yankeegroup.com

Europe

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
44-20-7307-1050 phone
44-20-7323-3747 fax
euroinfo@yankeegroup.com

Yankee Group | the global connectivity experts™

A global connectivity revolution is under way, transforming the way that businesses and consumers interact beyond anything we have experienced to date. The stakes are high, and there are new needs to be met while power shifts among traditional and new market entrants. Advice about technology change is everywhere—in the clamor of the media, the boardroom approaches of management consultants and the technology research community. Among these sources, Yankee Group stands out as the original and most respected source of deep insight and counsel for the builders, operators and users of connectivity solutions.

For 37 years, we have conducted primary research on the fundamental questions that chart the pace and nature of technology changes on networks, consumers and enterprises. Coupling professional expertise in communications development and deployment with hundreds of interviews and tens of thousands of data points each year, we provide qualitative and quantitative information to our clients in an insightful, timely, flexible and economic offering.

Yankee Group Link

As technology connects more people, places and things, players must confront challenging questions to benefit from the changes: which technologies, what economic models, which partners and what offerings? Yankee Group Link™ is the research membership uniquely positioned to bring you the focus, the depth, the history and the flexibility you need to answer these questions.

Yankee Group Link membership connects you to our qualitative analysis of the technologies, services and industries we assess in our research agenda charting global connectivity change. It also connects you to unique quantitative data from the dozens of annual surveys we conduct with thousands of enterprises and consumers, along with market adoption data, comprehensive forecasts and global regulatory dashboards.

Yankee Group Link Research

As a Link member, you have access to more than 500 research reports and notes that Yankee Group publishes each year. Link Research examines current business issues with a unique combination of knowledge and services. We explore topics in an easy-to-read, solutions-oriented format. With the combination of market-driven research and built-in direct access to Yankee Group analysts, you benefit from the interpretation and application of our research to your individual business requirements.

Yankee Group Link Interaction

Our analysts are at your further disposal with data, information or advice on a particular topic at the core of a Link membership. We encourage you to have direct interaction with analysts through ongoing conversations, conference calls and briefings.

Yankee Group Link Data

Yankee Group Link Data modules provide a comprehensive, quantitative perspective of global connectivity markets, technologies and the competitive landscape. Together with Link Research, data modules connect you to the information you need to make the most informed strategic and tactical business decisions.

Yankee Group Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and survey results to your specific needs to produce expert, timely, custom results.

Yankee Group Live!

The global connectivity revolution won't wait. Join our live debates to discuss the impact ubiquitous connectivity will have on your future. Yankee Group's signature events—conferences, webinars and speaking engagements—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this connectivity revolution.

www.yankeegroup.com

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel for builders, operators and users of connectivity solutions. For more than 35 years, Yankee Group has conducted primary research that charts the pace of technology change and its effect on networks, consumers and enterprises. Headquartered in Boston, Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific.